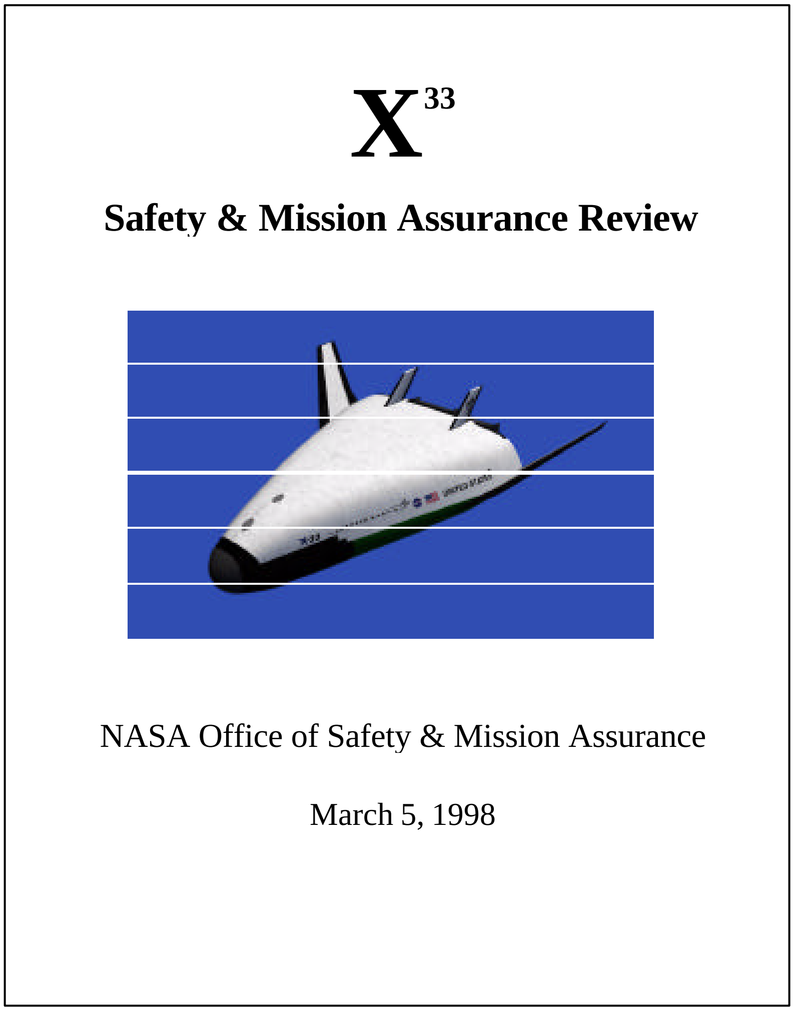
This document contains excerpts from the X-33 Independent Assessment Report (title page shown below). Only those sections which relate to the PBMA element **Hardware Design** are displayed.

The complete report is available through the PBMA web site, Program Profile tab.



X^{33}

Safety & Mission Assurance Review

NASA Office of Safety & Mission Assurance

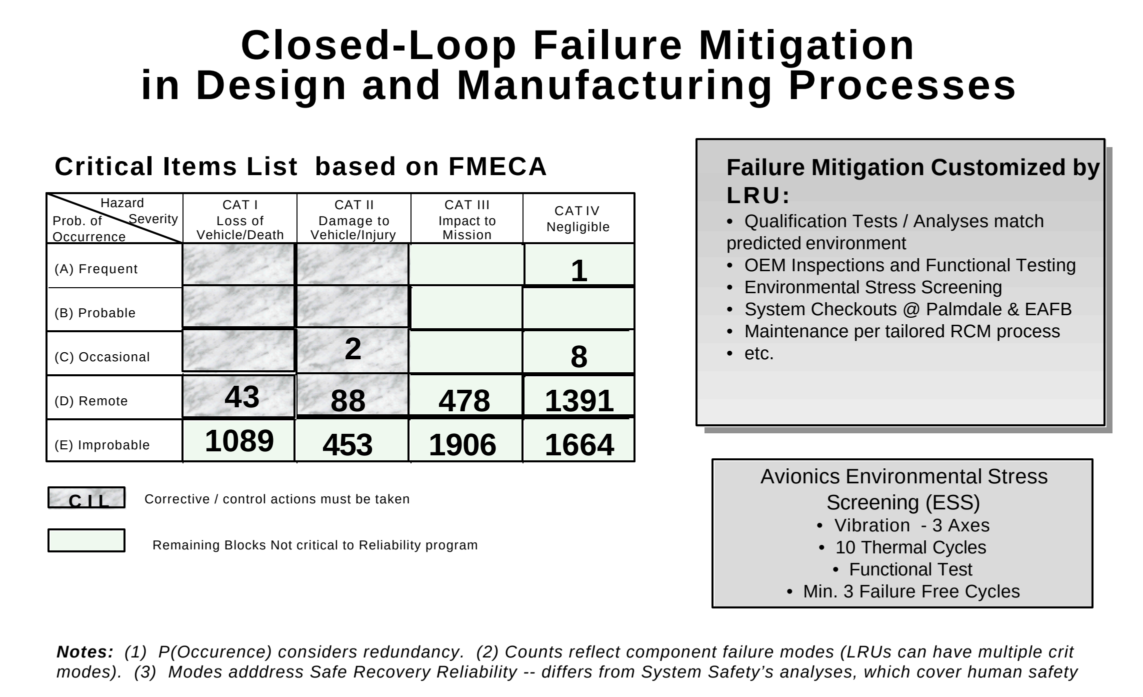
March 5, 1998

3.3 Hazard Analysis

The Hazard Analysis process has identified more than 1700 separate safety hazards. The self-contained Hazard Analysis System, supported by Failure Modes and Effects Analysis and Fault Tree Analysis activities identifies, evaluates, and mitigates safety risks. Safety risks are addressed in the Systems Safety Review Board management forum. It is the intent of the X-33 program to eliminate or mitigate all documented risks prior to the first flight. It was stated that 90 days prior to launch all hazards will be reviewed. All hazards will be closed out before flight.

3.4 Failure Modes and Effects Analysis (FMEA) Process

The X-33 program has implemented a rigorous use of the FMEA methodology in identifying and controlling risk. Potential weaknesses include the use of multiple formats in characterizing failure effects and inconsistency in the degree to which end-effects were estimated. A large number of Category 1E (critical but low probability) failure modes exist as shown in Figure 3.2 below.



Closed-Loop Failure Mitigation in Design and Manufacturing Processes

Critical Items List based on FMECA

Hazard Severity / Prob. of Occurrence	CAT I Loss of Vehicle/Death	CAT II Damage to Vehicle/Injury	CAT III Impact to Mission	CAT IV Negligible
(A) Frequent				1
(B) Probable				
(C) Occasional		2		8
(D) Remote	43	88	478	1391
(E) Improbable	1089	453	1906	1664

CIL Corrective / control actions must be taken

🟩 Remaining Blocks Not critical to Reliability program

Failure Mitigation Customized by LRU:

- Qualification Tests / Analyses match predicted environment
- OEM Inspections and Functional Testing
- Environmental Stress Screening
- System Checkouts @ Palmdale & EAFB
- Maintenance per tailored RCM process
- etc.

Avionics Environmental Stress Screening (ESS)

- Vibration - 3 Axes
- 10 Thermal Cycles
- Functional Test
- Min. 3 Failure Free Cycles

Notes: *(1) P(Occurence) considers redundancy. (2) Counts reflect component failure modes (LRUs can have multiple crit modes). (3) Modes adddress Safe Recovery Reliability -- differs from System Safety's analyses, which cover human safety*

Figure 3-2

Controversy exists concerning the tracking and aggregation of Category 1, and Category 2 failure modes with low probability of occurrence (Type E). Very few Critical Item List (CIL) issues (fewer than 10% of Cat-1 and Cat-2 failure modes) were reviewed at the Critical Design Review (CDR) as a result of this grouping strategy. The review team acknowledges that reviewing the Cat-1 and Cat-2 failure modes was not the sole purpose of the CDR. Nonetheless, the review team was concerned that the diminished visibility of these failure modes does not recognize the other uses of the CIL, such as formulating operating and maintenance procedures and mission rules. An independent observer at the SMA CDR noted: “If the current ground rules for Critical Items are continued, the X-33 Program management and NASA management will not be informed (have visibility) of all Loss of Vehicle/Death and Damage to Vehicle/Injury failure modes and interactions.”

Resolution

In discussions concerning this issue at the on-site review LMSW indicated that Category 1 hazards or failure modes “will not slip through the crack”. LMSW pointed to their computerized cross-referencing data base which identifies Critical Items on a system, sub-system, or component level for purposes of operations planning, maintenance, or other reasons. LMSW explained that the Cat-1 and Cat-2 failures get their own special attention, which includes quality acceptance and reliability centered maintenance. LMSW emphasized that they will not lose visibility of Category 1 items.

3.5 Fault Tree Analysis Process

The Fault Tree Analysis is one of the most powerful and widely used techniques of system safety on this program. Fault Tree Analyses were built and qualified for all critical X-33 components. There was evidence that probabilistic fault tree analyses were used to identify and rank critical failure combinations that lead to undesired outcomes. The technique was used to identify design changes in both hardware and software and to tailor operations and maintenance programs to eliminate or mitigate any additional issues identified downstream.